University of Oslo
INF3510 Information Security
Spring 2011
Workshop Questions

Lecture 12: Application and Operations Security

QUESTION 1

a. What are typical phases of operation of a virus or worm?
b. How does behavior-blocking software work?
c. In general terms, how does a worm propagate?

Answer

a. Dormant phase; Propagation phase; Triggering phase; Execution phase.
b. Behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.
c. Worms propagate by **1)** Searching for other systems to infect by examining host tables or similar repositories of remote system addresses. **2)** Establishing a connection with a remote system. **3)** Copying itself to the remote system and cause the copy to be run.

QUESTION 2

a. What is a botnet?
b. What is a DDoS, and how can a botnet be used to mount a DDoS attack?
c. Describer two other attacks that can be executed with botnet.

Answer

a. The term “botnet” is generally used to refer to a collection of compromised computers (called bots or zombie computers) running software, usually installed via drive-by downloads exploiting web browser vulnerabilities, worms, Trojan horses, or backdoors, under a common command-and-control infrastructure.
b. A denial of service (DoS) attack is an attempt to prevent legitimate users of a service from using that service. When this attack comes from a single host or network node, then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS attack. In a DDoS attack, an attacker is able to recruit a number of hosts throughout the Internet to simultaneously or in a coordinated fashion launch an attack upon the target. A botnet is precisely a set of hosts that can be coordinated for DDoS attacks.
c. Botnets are also used for spamming and for collecting identity credentials.

QUESTION 3

a. What is a buffer overflow attack, and how can it be prevented?
b. What is an SQL injection attack and how can it be prevented?
c. What is a Cross-Site Scripting attack, and how can it be prevented?

Answer

a. In computer security and programming, a buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash), or a breach of system security.
b. SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks can be prevented by not allowing user input to be directly embedded in SQL statements. Instead, parameterized statements must be used (preferred), or user input must be carefully escaped or filtered.
c. Cross-Site Scripting: (Acronym XSS) An attack technique that forces a web site to echo client-supplied data, which execute in a users web browser. When a user is Cross-Site Scripted, the attacker will have access to all web browser content (cookies, history, application version, etc). XSS attacks do not typically directly target the web server or application, but are rather aimed at the client. The web server is merely used as a conduit for the XSS data to be presented to the end client. XSS can be prevented by always sanitizing input to web servers.

QUESTION 4

Assume that Company A and Company B of similar size become victims of cyber attacks, and that as a result both companies suffer heavy damages that negatively affect customers and shareholders. When investigating the events it was found that Company A had practiced due dilligence and due care, whereas Company B had not. Assuming that the damages to both companies were equal, explain the possible differences, if any, in consequences and sanctions against management of the companies.

Answer

In general, management of companies is responsible for practicing prudent management, which means that they must practice due dilligence and due care. Management of Company B failed to do that, and could go to prison or be fined as a result, e.g. under the Sarbanes-Oxley act in the US, or the Basel II agreement in Europe.

QUESTION 5

Many things can go wrong when deploying new patches to systems.

a. List possible options for obtaining assurance that the patch comes from the correct source in the first place.

b. When a new patch is deployed to multiple systems, it is wise to update the systems in a sequence, not all at the same time. Explain why this is so.

Answer

a. Some options are:
   - Patch files can be signed, which would require key distribution (e.g. a PKI) to validate the signatures.
   - The patch files can be accompanied with a checksum, where at the same time the checksums are distributed through independent and/or secure channels.
   - Get the patches through independend and/or secure channel.

b. Implement patches to the least sensitive systems first,wait and see if the change was successful and did not have any negative consequences, and then deploy the patched to the most sensitive systems last. When something goes wrong this principle minimizes negative consequences.